OSD CLOUD MIGRATION PRIMER

March 2025

Executive Summary

In today's rapidly evolving digital landscape, the Office of the Secretary of Defense (OSD) must embrace innovative technologies to stay competitive and to drive successful mission outcomes. Cloud computing is a cornerstone of this digital transformation, offering flexibility, scalability, and cost efficiency. Migrating mission systems to the cloud enables OSD organizations to modernize their information technology (IT) infrastructures, enhance operational efficiency, and quickly adapt to new or evolving mission requirements.

This OSD Cloud Migration Primer builds upon the OSD Cloud Migration Vision and consolidates relevant Department of Defense (DoD) policy guidance and requirements into an OSD mission-focused cloud migration methodology based on technology and business inputs. It was developed with input from the cloud-focused sections within the DoD's Software Modernization Strategy, the DoD Cloud FinOps Strategy, the General Services Administration's (GSA) Modernization and Migration Management (M3) Framework, and input from the OSD IT enterprise customer base. This primer and the forthcoming OSD Cloud Migration Playbook will support and enable OSD organizations to identify, assess, and decide what and when to transition OSD data, applications, and services from legacy on-premises infrastructure to cloud capabilities. The playbook will leverage the DoD Cloud Community of Interest to help identify best practices, internal roadblocks, and policy gaps organizations may face – and must overcome – as they transition from on-premises to the cloud. It will also provide repeatable processes within an approved framework for OSD organizations to utilize while embarking on their cloud migration journeys. The OSD Chief Information Officer (CIO) cloud migration efforts will fulfill the DoD Cloud Strategy's (2018) requirement for organizations to "create repeatable migration processes" and align with FY26-FY30 OSD IT Digital Modernization Roadmap goals, the DoD IT Advancement Strategy called Fulcrum, and DoD policies.

The OSD CIO has created the OSD Cloud Migration Primer to inform, engage, and unify OSD organizations as they enter a new era of innovation and agility from cloud computing. This primer intends to spark meaningful dialogue on cloud migrations within the OSD framework—encouraging organizations to consider how these migrations will work, why they are essential, and what challenges they may face or have already encountered. By fostering discussion and knowledge-sharing, the primer helps organizations formulate high-level strategies for the forthcoming playbook's more operational, business-oriented guidance. By harnessing the transformative power of cloud computing, OSD CIO's goal is to help guide and unify OSD's digital transformation, ensuring OSD remains at the forefront of technological advancements. This initiative is about more than migrating to the cloud – it is about creating a continuous learning and improvement culture within OSD that enables OSD to stay ahead of the curve and adapt to the ever-changing technology landscape. By embracing cloud computing, OSD will unlock enhanced speed and agility, improve security capabilities, and enable rapid responses to new threats and opportunities.

Table of Contents

Vision

Per the OSD Cloud Migration Strategic Vision, signed in October 2024, *"OSD's cloud migration strategy will enable a consistent, secure, and efficient transition of mission-critical applications and data to the cloud while minimizing disruption to ongoing operations and ensuring the highest levels of security and compliance."*

Mission

The OSD CIO cloud migration mission is to empower OSD organizations to achieve their strategic objectives and initiatives by supporting successful migration to modern cloud capabilities, establishing effective governance, and removing obstacles to innovation. The objective focuses on creating an agile and collaborative culture that prioritizes continuous improvement so OSD organizations can adopt advanced technologies and standardize their business processes and best practices to achieve superior outcomes.

Objectives

The FY26-FY30 OSD IT Digital Modernization Roadmap set forth an ambitious plan to change defense IT systems. The transformation opens significant opportunities for OSD organizations to integrate advanced technologies like artificial intelligence and machine learning into their automated processes. Achieving this vision starts with successful cloud migration. According to the roadmap details, the OSD CIO seeks to boost cloud migration to reach a 50% increase by Fiscal Year (FY) 2028.

This Cloud Migration Primer serves as a guide to help organizations unlock the full potential of cloud computing. It provides essential background information on OSD's planned cloud journey. Organizations that apply the instructions from this primer and the future playbook will successfully manage cloud migration obstacles and seize available opportunities. This guide reduces risks through its structured framework to manage potential challenges and achieve a safer and smoother cloud migration process.

The primary objectives of OSD CIO's cloud migration efforts are to (1) enable migrations, (2) reduce risk, and (3) formalize governance. This primer also identifies near-term (FY2025) focus areas for OSD CIO, including formalizing OSD cloud governance, developing the playbook, and executing OSD cloud migration pilots to refine the playbook.

Enable Migrations

The OSD's adoption of cloud technology will enhance security and operations while boosting mission readiness through advanced technological capabilities. The objective is to establish repeatable processes utilizing migration phases aligning with DoD standards, federal guidelines, and industry best practices. To accomplish this, the OSD CIO will develop a cohesive Cloud Migration Playbook in FY2025 that provides a framework for OSD organizations to execute their cloud migrations. By meeting this objective, the OSD stands to gain numerous cloud computing advantages, such as strengthened security and privacy, better scalability, and faster operational agility, which will benefit its essential missions.

The OSD Cloud Migration Playbook will be an interactive and scalable resource designed to help OSD organizations assess and identify appropriate applications, data, and services for cloud migration. Adhering to DoD standards and aligning with the National Institute of Standards and Technology (NIST) Risk Management Framework, the playbook applies security and privacy controls as required by NIST Special Publication (SP) 800-53. It incorporates industry best practices to ensure a structured and efficient migration process. The playbook outlines a structured step-by-step cloud migration process encompassing assessment and planning stages through execution and post-migration activities to guide organizations through migration complexities.

The OSD Cloud Migration Playbook primarily supports OSD leaders and managers in making informed decisions for their organizations' smooth transitions to cloud capabilities rather than serving as a technical how-to guide. Organizations consistently report that business processes and requirements—not technical challenges—are the most significant

roadblocks to successful and timely migrations. The playbook addresses this gap by delivering essential strategic and operational direction to overcome challenges while maximizing organizational benefits from cloud adoption through efficient practices. This leadership-focused approach is critical for successful cloud migrations with minimal disruptions to business operations while ensuring a secure, scalable, and agile cloud environment supporting mission-critical operations.

Reduce Risk

Cloud migrations can be complex and fraught with risk, but leveraging industry best practices, existing frameworks, and insights from prior migrations can significantly reduce the likelihood of errors, disruptions, and security and privacy incidents. To achieve this, OSD CIO will leverage the OSD Cloud Migration Playbook and its associated resources to support OSD organizations as they:

- *Conduct thorough risk assessments:* Identify potential risks and vulnerabilities associated with the migration, such as data loss, downtime, security, and privacy threats.
- *Develop a comprehensive risk mitigation strategy:* Based on the risk assessment, develop a strategy to mitigate or eliminate identified risks, including implementing security and privacy controls, data backup and recovery processes, and Continuity of Operations (COOP) and contingency plans.
- *Monitor and report on migration progress:* Track key performance indicators (KPIs) and metrics to measure the migration's success, identify areas for improvement, and make data-driven decisions.
- *Leverage best practices and frameworks:* Use established cloud migration frameworks, such as the Cloud Security Alliance's (CSA) Cloud Controls Matrix (CCM) and the NIST Cloud Computing Reference Architecture (CCRA), to direct the migration process while maintaining adherence to industry standards.
- *Incorporate lessons learned from prior migrations:* Analyze the successes and challenges of previous cloud migrations, both within the organization and in the industry, to identify areas for improvement and opportunities for optimization.
- *Solicit expert feedback and guidance:* Connect with cloud migration professionals, such as vendors, consultants, and peers, to obtain valuable insights and best practices for managing the migration process effectively.
- *Implement a phased migration approach:* Consolidate the migration process into smaller phases, enabling teams to perform testing and validation and make iterations to lower both disruption and risk.
- *Establish clear communication and collaboration channels:* Foster open communication and collaboration among stakeholders, including IT teams, business units, and external partners, to ensure everyone is aligned and informed throughout the migration process.
- *Conduct regular security, privacy, and compliance audits:* Consistent audits should be performed to verify that the migrated environment satisfies security, privacy, and compliance standards and implement necessary changes.
- *Develop a post-migration review and evaluation process:* Conduct a detailed examination of the migration process to discover valuable insights, areas needing enhancement, and potential future optimization opportunities.

Formalize Governance

To ensure a successful and secure cloud migration, OSD requires cloud governance. Governance will guide and support OSD organizations throughout their cloud journeys while keeping the greater OSD IT enterprise informed and aware. In FY2025, OSD CIO will play a critical role in formalizing governance for cloud migrations by:

- *Participating in DoD cloud governance oversight teams:* Actively engage with existing DoD cloud governance oversight teams to provide OSD organizations with implementation guidance, best practices, and lessons learned from previous cloud migrations.
- *Establishing an internal OSD Cloud Governance Committee:* This committee will bring together representatives from OSD organizations, the DoD CIO, the DoD Senior Agency Official for Privacy (SAOP), and other relevant stakeholders to provide strategic guidance and oversight on cloud migration efforts.

- *Conducting an application and services inventory:* Partner with the DoD CIO to facilitate an inventory of existing and planned applications and services identified for cloud migration by OSD organizations. This inventory will help to:
    - Gain efficiencies in capability delivery by identifying opportunities for consolidation and optimization.
    - Identify potential cost savings by streamlining business practices and services portfolios.
    - Ensure that resources are utilized effectively and aligned with mission objectives.
    - Ensure compliance readiness with H.R. 5009 DoD Cloud Computing Capabilities (Sec. 1505).

The OSD cloud governance framework will align cloud migration activities with OSD mission objectives, along with DoD policies and industry best practices. OSD organizations can securely and effectively manage cloud migration complexities through formalized cloud governance while efficiently transitioning to the cloud.

Guiding Principles

The OSD Cloud Migration Primer follows and consolidates the guiding strategy, principles, and policies outlined in the DoD Cloud Strategy, FY26-FY30 OSD IT Digital Modernization Roadmap, goals within the DoD IT Advancement Strategy known as Fulcrum, DoD Zero Trust Strategy, and other DoD strategies. They identify modular approaches for cloud migrations that are streamlined, efficient, and mission oriented. The principles enable OSD to evolve from isolated systems into contemporary cloud solutions. *Appendix A* contains the guiding principles that draw their foundation from pre-existing DoD policies and previous cloud migration experiences. They aim to eliminate uncertainties and assumptions and mitigate risk to maintain cloud migration schedules.

Next Steps

Cloud Migration Playbook

In FY2025, OSD CIO will develop and publish a comprehensive Cloud Migration Playbook to ensure smooth and secure cloud migrations. This dynamic resource will serve as a framework for all OSD cloud migrations, providing:

- *A Phased Approach:* The playbook maps out clear steps to move on-premises data and systems alongside applications to approved secure cloud environments through manageable phases. A structured approach creates a migration process that remains controlled, predictable, and repeatable.
- *Best Practices and Checklists:* The playbook will include practical guidance and checklists based on industry best practices and previous OSD and DoD cloud migration experiences. These resources will ensure security protocol compliance and optimize resource distribution while reducing disruptions.
- *Collaborative Knowledge Sharing:* The playbook will function as a platform to document and distribute insights and solutions as well as lessons learned throughout the OSD and DoD cloud community. This collaborative approach facilitates knowledge sharing while accelerating problem resolution and encouraging ongoing enhancements.
- *Dynamic and Evolving Resources:* The playbook is designed to be adaptable to keep pace with the constantly shifting cloud technology landscape and its best practices. It will have an online presence and be maintained through ongoing updates. The approach remains an up-to-date, valuable information resource, integrating the most recent insights and tools to support the success of cloud migration.

Additional details can be found in Appendix B.

Pilot Migrations

Before a full-scale rollout of the Cloud Migration Playbook, OSD CIO will coordinate strategic pilot migrations with select OSD organizations. These pilots are critical opportunities to gain practical experience, collect data, and refine the migration process. They are designed to:

- *Validate and Refine the Playbook:* The Cloud Migration Playbook will be tested in actual situations through pilot migrations. Pilot feedback will be used to enhance the playbook's guidance and ensure that it remains practical and effective for every subsequent migration.
- *Mitigate Risk Proactively:* Pilot migrations will help reduce implementation risks by early identification and resolution of potential problems within controlled environments. This strategy enables OSD organizations to transition smoothly and predictably.
- *Build Confidence and Expertise:* Through successful pilot migrations, the OSD proves the feasibility and benefits of cloud adoption, which generates stakeholder trust while promoting broader organizational adoption. Teams involved in the process acquire essential practical knowledge, which they can disseminate throughout their organization.
- *Optimize for Performance and Security:* Through pilot migrations, organizations can thoroughly assess and improve the effectiveness of their migration technologies and tools. These evaluations enable teams to check cloud service performance practically while discovering security weaknesses and maintaining strict security compliance.
- *Quantify Tangible Benefits:* Pilot migrations provide concrete data to measure the benefits of cloud migration. This includes quantifying cost savings, demonstrating increased efficiency and agility, and highlighting improvements in data security and disaster recovery capabilities.

The Cloud Migration Playbook and strategic pilot programs establish a robust framework to guarantee secure and efficient cloud migration success throughout the OSD enterprise. The department achieves complete cloud computing capabilities through a dual approach based on teamwork and relentless enhancement.

Call to Action

This Cloud Migration Primer is a call to action for all OSD organizations to embrace the cloud and to:

- *Understand the "Why":* Internalize the critical need for cloud migration in shaping OSD's future, as detailed in the Digital Modernization Roadmap and emphasized throughout this primer. Legacy and siloed IT systems prevent OSD from becoming the modern, agile, and data-driven organization needed for the 21st century. Cloud migration unlocks key benefits like enhanced security, efficiency, and access to cutting-edge technologies.
- *Prepare for Action:* Become familiar with this primer's guiding principles, strategies, and best practices. While the Department has embraced cloud computing in many areas, and the DoD Joint Warfighting Cloud Capabilities (JWCC) contract has improved access to cloud services, numerous OSD IT enterprise services and products – including critical defense business systems – have yet to transition fully. Begin assessing your organization's IT infrastructure and identifying potential challenges and opportunities for cloud migration. Build a dedicated team and allocate the necessary resources to support a successful migration process.
- *Engage with the Process:* Building a Cloud Migration Playbook must be a collaborative effort, and just like the cloud migration itself, cannot be done in a silo. The expertise and engagement of OSD organizations are critical to the success of the playbook and future cloud migrations.
    - Participate and engage with communities of interest and monitor others navigating their own cloud migrations.
    - The DoD CIO Cloud Rationalization Working Group is actively collecting information on cloud contracts across the Department, assisting organizations in transitioning to JWCC or other authorized enterprise contracts and reporting to the DoD CIO Enterprise Cloud Management Board to fulfill the FY25 National Defense Authorization Act (NDAA) Section 1505 requirements for Congress. As such, it is important to start

analyzing, assessing, and documenting current legacy systems to look for gaps and redundancies, security and privacy challenges, and system dependencies.
    - Engage through Correspondence and Task Management System (CATMS) to help develop this Primer and the upcoming Cloud Migration Playbook.
- *Embrace Continuous Improvement:* Lead the charge for cloud adoption and demonstrate its powerful transformation capabilities. Cloud migration is a continuous process rather than a single event. Track performance metrics while optimizing resource distribution and staying adaptable to changes in the cloud environment. Building an organizational culture that values learning, teamwork, and innovative thinking will help you fully exploit cloud computing advantages. Utilize this primer to guide your organization through essential changes while promoting positive transformations.

Conclusion

The OSD has confirmed that migrating to cloud represents a significant transformation that provides exceptional possibilities to improve operational efficiency, security, and privacy while boosting organizational agility. OSD organizations gain access to scalable resources available on-demand through cloud capabilities, which enable fast decision making and support essential mission operations. Through cloud services, OSD organizations achieve uninterrupted internal and external collaboration while ensuring their personnel always maintain access to essential tools and information from any location.

The OSD Cloud Migration Primer highlights cloud technology as an essential tool for collaboration, which creates a unified platform for cross-organization operations and real-time coordination alongside knowledge sharing. Effective cooperation between OSD organizations enhances their ability to respond to evolving mission demands or requirements. This document presents an overarching strategy for transforming OSD's IT systems to eliminate silos while building partnership networks and encouraging innovative practices that prioritize security and privacy without reducing operational efficiency.

In the increasingly complex and interconnected global security environment, cloud adoption is not just a technological upgrade but an essential investment in OSD's ability to respond to crises and maintain a competitive technological edge. The methodology laid out in this primer is designed to ensure OSD organizations have a successful and smooth migration to the cloud and to significantly enhance OSD's ability to deploy resources quickly and efficiently, ensuring that OSD can respond effectively to immediate operational needs and long-term strategic objectives. Embracing cloud migration will ensure that OSD remains a formidable force today and a beacon of technological advancement on tomorrow's battlefield.

Appendix A: Guiding Principles

DoD Cloud Strategy - Cloud Smart

Cloud Smart is a strategy for adopting cloud technology. It is designed to leverage cloud computing to improve the DoD's warfighting capabilities, enhance cybersecurity, and optimize IT operations. Cloud Smart is built on four pillars:

- *Security:* Cloud computing prioritizes security and privacy. The strategy demands strong security and privacy protection measures to safeguard sensitive cloud systems and information.
- *Data:* The strategic approach prioritizes the proper management, storage, and protection of data as it represents a fundamental asset held in the cloud.
- *Cloud Infrastructure:* The strategy acknowledges the need for strong and durable cloud infrastructure. To maintain flexibility and prevent vendor dependency, organizations should use multiple cloud providers and a hybrid approach.
- *Services:* The strategy identifies cloud services that address specific requirements to support warfighting operations, intelligence work, and other essential missions.

DoD Cloud Strategy - Data Smart

The DoD Data Smart Strategy represents a data management approach aimed at enhancing DoD's data collection methods and its storage and data usage governance practices. The DoD launched this initiative in 2020 to support its dedication to data-driven decision making and operational analytics. The fundamental principles that form the foundation of the Data Smart Strategy include:

- *Data as a Strategic Asset:* Data operates as a vital asset that supports decision-making processes, optimizes operations, and boosts warfighting performance.
- *Data Standardization:* Create uniform data formats and structures throughout the Department to enable efficient data sharing and utilization.
- *Data Sharing:* Encourage legal data sharing between organizations and systems to eliminate barriers and enhance teamwork.
- *Data Analytics:* Building advanced data analytics capabilities will give analysts and decision makers better insights from extensive datasets.
- *Data Security and Privacy:* Prioritize data security and privacy to protect sensitive information from cyber threats and unauthorized access.

Data Smart delivers efficient data management solutions to help streamline OSD cloud migration processes. OSD's strategic approach to data assets enables it to enhance operational efficiency and decision making through cloud technology utilization. Effective data management is essential for mission success because standard data practices improve teamwork while strengthening data analysis and safeguarding sensitive information during cloud migrations.

Zero Trust

The DoD Zero Trust strategy is an approach to cybersecurity that assumes all users and devices are potential threats. Implementing a Zero Trust architecture is designed to protect DoD's information and systems from threats. The key principles are:

- *Default Deny:* All traffic is denied by default, and access is only granted on a need-to-know basis.
- *Least Privilege:* Users and devices are granted the minimum level of access necessary to perform their functions.
- *Micro-Segmentation:* The network is divided into smaller, isolated segments to limit the spread of malware and unauthorized access.
- *Continuous Verification:* Users and devices are continuously monitored and verified to ensure they remain authorized and trustworthy.
- *Data-Centric Security:* Data is always protected, regardless of where it is stored or transmitted.

Appendix B: Cloud Migration Playbook

OSD CIO intends to develop and publish a Cloud Migration Playbook in FY2025. The playbook will outline a phased process for migrating on-premises infrastructure to approved secure cloud environments. It will incorporate insights and suggestions derived from lessons learned by both OSD and other DoD organizations that have migrated to the cloud. The playbook will delineate steps and processes that enabled those organizations to have successful outcomes. Each phase of the migration framework – described below – is essential, and OSD organizations should follow the phases in sequence.

Assessment

In the assessment phase, OSD organizations perform thorough evaluations to decide whether their applications can be moved to cloud environments. Successful cloud migration depends on this phase, which helps identify potential obstacles alongside opportunities and necessary requirements. Key activities include:

1. **Develop Business Case:**
   - Clearly articulate the objectives and benefits of moving to the cloud (e.g., cost savings, scalability, improved agility) and the cost of migration and maintenance for the planning phase.
   - Define the scope, timeline, and budget for the migration project.
   - Establish KPIs to measure the success of the migration.
2. **Budget, Estimate Costs, and Estimate Savings:**
   - Estimate costs associated with migration, including infrastructure, labor, and potential third-party costs.
   - Calculate potential savings from moving to the cloud, such as reduced capital expenditures, operational expenses, and energy consumption.
   - Consider cloud-based solutions' total cost of ownership and return on investment.
3. **Define Roles and Responsibilities:**
   - Identify stakeholders and establish roles and responsibilities.
   - Define communication channels and protocols for collaboration and issue escalation.
4. **Identify Existing Assets:**
   - Catalog all IT assets, including:
     - Hardware (e.g., servers, storage, network devices).
     - Software (e.g., applications, licenses, dependencies).
     - Applications (e.g., custom-developed, third-party, legacy).
5. **Analyze Current Cloud Data and Workloads:**
   - Analyze the data and workloads of the current cloud, if applicable.
   - Assess the viability of workloads for achieving performance, scalability, and cost effectiveness in the cloud.
   - Identify potential bottlenecks, dependencies, and areas for optimization.
6. **Identify Legacy Systems:**
   - Identify legacy systems that need to be upgraded, replaced, or refactored.
   - Assess the complexity, cost, and risk associated with modernizing.
   - Identify operational requirements for the current system and network environment.
   - Identify concept of operations (CONOPS), including operational benefits and risk, for employing the system within a cloud environment.
   - Identify threats and vulnerabilities associated with migration and employment, such as data loss, downtime, and security.
   - Identify risk mitigation strategies, including security controls, data backup, resiliency and recovery processes, and contingency plans.
7. **Understand Dependencies:**
   - Assess interdependencies among applications to plan migration phases effectively.

8. **Assess Data Sensitivity**
    - Identify the sensitivity of the data processed by the application under consideration for migration.
    - Identify the data types of the application processes.
    - Review those data types in consultation with appropriate stakeholders to determine their sensitivity.
        - For example, consult with the Senior Component Official for Privacy regarding data containing personally identifiable information.
    - Determine which cloud computing environment is most appropriate for processing the data contained in the application.
9. **Define Risks and Roadblocks:**
    - Identify potential risks, roadblocks, and challenges that could impact the migration.
    - Assess the likelihood, impact, and mitigation strategies for each risk.
    - Develop a risk management plan to address potential issues and ensure a smooth migration process.

Planning

During the planning phase, organizations utilize the data captured during the assessment phase to formulate a comprehensive migration plan. This phase involves defining a clear organization-specific migration strategy, crafting a migration roadmap, designing the target architecture, identifying cloud service providers, ensuring security, privacy, and other compliance, planning performance, and planning an exit strategy. Key activities include:

1. **Define Migration Strategy:**
    - Set clear objectives for the migration, including measures of success.
    - Establish a migration framework that outlines the scope, timeline, budget, and resources required.
    - Define the migration approach, including the type of migration (i.e., lift-and-shift, re-architecture, hybrid), the migration sequence, and the dependencies involved.
2. **Identify Cloud Service Provider(s):**
    - Research and evaluate potential cloud service providers based on cost, security, and privacy compliance.
    - Assess the cloud service provider's experience, expertise, and track record in supporting similar migrations.
    - Evaluate the cloud service provider's security and privacy controls, compliance certifications, and regulatory adherence.
3. **Design the Target Architecture:**
    - Construct the architecture of the future cloud environment that fulfills performance, security, and privacy requirements.
    - Define the cloud service model (i.e., infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), software-as-a-service (SaaS)), deployment model (i.e., public, private, hybrid), and cloud service provider(s) to be used.
    - Ensure the target architecture aligns with the organization's business objectives, security and privacy requirements, and compliance standards.
4. **Craft a Migration Roadmap:**
    - Develop a detailed timeline and sequence for migrating workloads, including the dependencies involved and available resources.
    - Identify critical milestones, deadlines, and checkpoints to ensure the migration stays on track.
    - Establish a resource allocation plan to ensure sufficient personnel, infrastructure, and budget are available to support the migration.
5. **Ensure Security and Privacy Compliance:**
    - Comply with relevant regulations and standards, such as the Federal Risk and Authorization Management Program (FedRAMP) and the Cloud Computing Security Requirements Guide (CC SRG).
    - Implement security and privacy controls and measures as required by NIST SP 800-53 to protect sensitive data and ensure the confidentiality, integrity, and availability of cloud-based assets.

- Ensure compliance with all required DoD policies and Federal regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), the DoD Privacy Act Policy (DoD Directive 5400.11), and the DoD Cybersecurity Policy (DoD Instruction 8500.01).

6. **Evaluate IT Staff**
   With organizations transitioning to the cloud, evaluating their IT team's capacity to handle the transition and future operations is imperative. Conducting an audit enables leaders to find gaps in skills and determine whether training, retraining, or hiring new employees is needed. Conduct a skills assessment to determine where staff are lacking and where improvements can be made in the following areas:
   - Cloud platform knowledge: Experience with the selected cloud platform (e.g., AWS, Azure, Google Cloud).
   - Security and Compliance: Knowledge of cloud security standards and compliance requirements.
   - Cloud design and architecture: Knowledge of cloud architecture and design concepts.
   - Cloud management and operations: Experience with cloud management tools and platforms.

   Based on the assessment, create a training plan to fill in gaps and create learning opportunities and seek out additional resources, if necessary, for specialized work or extra demand.
7. **Plan Performance:**
   - Utilize specific, measurable, achievable, relevant, and time-bound (SMART) goals, feedback mechanisms, and stakeholder engagement to set realistic targets and monitor progress toward those targets.
     - SMART Goals: Use SMART goals to evaluate migration efforts. Check in regularly to see how progress compares to benchmarks.
     - Feedback Mechanisms: Build feedback loops from operational users to improve the cloud services incrementally based on real-world experience.
     - Stakeholder Engagement: Identify key stakeholders, agree on objectives, and inform them of the migration strategy.
8. **Plan Exit Strategy:**
   Build exit triggers into the strategy to plan for circumstances like the following:
   - Cost Increases: Major increases in costs or negative changes may require a re-evaluation if cloud costs move far beyond the budget.
   - Performance Issues: Performance problems are ongoing and constant. If the number or severity of these issues becomes unmanageable, they interfere with business operations.
   - Security or Privacy Concerns: If sensitive data is involved and security or privacy is inadequate, an emergent security or privacy risk or weakness in the cloud must trigger the exit.
   - Policy Directive: If a policy or directive change prevents further migration to the cloud, then an assessment and review of existing services should be conducted to determine necessary adjustments or alternatives.

Execution

The Execution phase is the most critical stage of the OSD migration process. It is where the actual migration of workloads to the cloud takes place. This phase involves key activities that ensure a smooth transition of applications, data, and services to the cloud environment.

1. **Prepare the Cloud Environment:** Set up the cloud infrastructure and services required to run migrated workloads, ensuring DoD cloud computing security requirements are met.
2. **Migrate Data:** Transfer data to the cloud, ensuring integrity, security, and privacy.
3. **Migrate Applications:** Migrate applications and test the workload. Verify workloads are running correctly.
4. **Monitor Migration:** Monitor performance during migration and troubleshoot any problems that arise.

Post-Migration

Once migration is complete, organizations enter the post-migration phase, focusing on stabilization and integration. Key activities include:

1. **Validate and Test:** Ensure applications function properly after relocation to the new environment.
2. **Monitor Performance:** Conduct a performance analysis of the application to see how it responds to the allocated resources and what can be done to reassess or optimize those resource allocations.
3. **Offer Training and Support for Users:** Train staff on new systems and processes for operating in the cloud environment.

Optimization

In the final step of the framework, organizations fine-tune their cloud deployments. Key activities include:

1. **Continuously Improve:** Embrace and constantly evaluate performance metrics to identify opportunities for improved usage and application performance. This proactive approach puts organizations in control of their cloud deployments.
2. **Manage Costs:** Review usage patterns in the cloud for cost analysis and forecasting.
3. **Scale Resources:** Scale resources according to usage patterns (e.g., scale up or down based on business needs).

By following these phases, which can be repeated for multiple iterations, organizations can effectively migrate to cloud environments while taking advantage of the cloud's cost savings, performance improvement, and increased organizational agility.